홈네트워크에서 DHCP 메시지 인증에 관한 연구

주홍일* · 황진범* · 한종욱*

*한국전자통신연구원 홈네트워크보안연구팀

A study of the DHCP message authentication at home network

Hong-il Ju* · JinBum Hwang* · Jong-wook Han*

*Home Network Security Research Team, ETRI

E-mail : juhong@etri.re.kr

요 약

본 논문은 DHCP(Dynamic Host Configuration Protocol) 메시지 인증에 관한 것으로 홈네트워크에서 적용 가능한 디바이스 인증 및 사용자 인증과의 관련성에 대해 살펴본다. 또한, 본 논문에서 제안하는 DHCP 메시지 인증은 DHCP 서버가 IP 주소 할당을 요구하는 DHCP 클라이언트들에게 IP 주소를 할당함에 있어서, 인증 과정을 거친 후 인증에 성공한 클라이언트에게만 IP 주소를 할당 해주고, DHCP 클라이언트도 자신이 등록된 DHCP 서버로부터만 IP 주소를 할당 받을 수 있는 DHCP 메시지 인증 방법을 제안함에 있어서 효과적이고 보안성을 강화한 키관리 방법으로 리플레이 공격에 대한 방지법을 포함하는 DHCP 메시지 인증 방법을 제공한다.

키워드

홈네트워크, DHCP, 인증, 키관리, 리플레이 어택

Ⅰ. 서 론

최근 무선 인터넷과 이동통신 시스템의 발달로 노트북, PDA 등과 같은 이동 단말기를 사용하는 이용자들이 급증하고 있으며, 이러한 대부분의 사용자들은 언제 어디서나 인터넷에 접속하기를 원한다. 그러나, 이러한 이동 단말기가 원활한 인터넷 서비스를 제공하기 위해서는 네트워크 서비스 지역을 옮길 때마다 IP 주소, 게이트웨이, 네임서버 등을 포함한 시스템 환경이 자동적으로 변경되는 등의 서비스 지원이 요구된다. DHCP는 이러한 IP 설정 및 서브넷 마스크의 설정 등을 포함하여 자동적으로 할당해주는 프로토콜 중 하나이다[1].

또한, 최근 가정 내 PC 보급률의 증가와 인터넷 이용자의 폭발적인 증가 및 인터넷 정보가전 기기의 등장으로 인해 댁내 정보화가 중요한 이슈로 인식되고 있으며, 이와 더불어 유비쿼터스 및 홈네트워크에 대한 관심도 고조되고 있다. 이미 홈네트워크를 구현한 사이버 아파트가 등장하고 있다. 홈네트워크는 가정내의 다양한 정보가전 제품을 유무선 통신 네트워크로 상호 연결하여, 네트워크에 연결된 모든 기기들을 시간이나 장소에 구애 받지 않고 원격 제어 및 멀티미디어 서비스 등 다양한 서비스를 가능하게 한다. 이러 홈네트워크의 성공적인 홈네트워크 산업의 활성화를 위해서는 홈네트워크 보안 기술이 반드시 해결되어야 할 필수 요소로 거론되고 있다. 홈네트워크의 보안을 위해서는 먼저 디바이스인증 및 사용자 인증 과정을 통해 정당한 디바이스와 정당한 사용자만이 홈네트워크에 접근할 수 있도록 해야 하며, 인증된 사용자라 할지라도 접근권한에 따라 서비스의 차별화가 이루어져야 한다[2-3]. 따라서, 본 논문에서는 이러한 홈네트워크 보안 기술을 위해 적용 가능한 DHCP 메시지 인증에 대해 기술하고자 한다.

본 논문의 구성은 1절에서 서론을 간략히 기술하고, 2절에서는 DHCP의 개요, 3절에서는 DHCP 메시지의 인증, 4절에서는 홈네트워크 보안에서의 DHCP에 대해 언급하고, 마지막 5절에서 결론을 기술한다.

Ⅱ. DHCP의 개요

DHCP란 호스트 등의 IP주소 설정 시 사용자가 고정적으로 IP주소를 할당하지 않고, DHCP 서버가 제공하는 IP 주소, 서브넷 마스크, 게이트웨이, DNS 등의 정보를 자동으로 할당 받을 수 있는 기능이다. 이는 사용자가 각 컴퓨터에 직접 IP주소를 비롯한 TCP/IP설정을 입력하지 않아도 되고, 잘못된 IP 주소 지정으로 인한 오류도 방지하며, DNS와 Wins 서버의 주소를 포함한 네트워크 주요 구성 정보가 바뀌어도 클라이언트를 위

한 추가 작업 불필요하다. 또한, 네트워크 관리자는 많은 클라이언트가 존재하는 네트워크 구성에서 효율적으로 IP 관리가 가능하다.

2.1 DHCP의 동작 과정

DHCP의 동작 원리는 DHCP 클라이언트가 시스템이 시작됨과 동시에 DHCP 서버를 찾는 메시지를 네트워크에 발송하여 IP 주소 할당을 요청하게 되며, DHCP 서버는 이러한 클라이언트의 요청에 응답하여 자신의 DHCP Database에서 IP 주소를 할당해 준다. DHCP 클라이언트가 새로운 IP 주소를 할당 받기위한 동작 과정은 아래와 같으며, 그림 1은 DHCP 클라이언트의 초기화 및 네트워크 주소 할당 과정을 보여준다[4].

1) DHCP 클라이언트는 INIT 상태에서 시작하며 IP 주소를 할당받기 위해DHCPDISCOVER 메시지를 broadcast한다.
2) DHCPDISCOVER 메시지를 수신한 DHCP 서버는 DHCPOFFER 메시지의 제공 여부를 결정하며, 응답시 *yiaddr* 필드에 가용한 IP 주소를 담아서 broadcast한다.
3) DHCP 클라이언트가 다수의 DHCPOFFER 메시지를 수신하면 하나의 DHCP 서버만 선택하며, 선택된 DHCP 서버가 제공한 IP 주소를 DHCPREQUEST 메시지의 *Server identifier* 옵션 필드에 담아서 서버에게 broadcast한다.
4) DHCP 서버가 *Server identifier* 옵션 필드를 검사하여 자신의 주소와 일치하면 DHCPACK 메시지(주소가 가용한 경우)나 DHCPNAK 메시지(이미 할당된 경우)를 전송한다.
5) DHCPACK 메시지를 수신한 DHCP 클라이언트는 할당된 IP 주소를 사용할 수 있으며, DHCPNAK 메시지를 수신하면 1)번 과정부터 반복한다.
6) 할당된 주소에 문제가 있을 경우, DHCP 클라이언트는 DHCP 서버에게 DHCPDECLINE 메시지를 송신하고 1)번 과정부터 반복한다.
7) DHCP 클라이언트는 주소 임대 기간이 종료되기 전이라도 DHCPRELEASE 메시지를 이용하여 할당된 IP 주소를 반환할 수 있다.

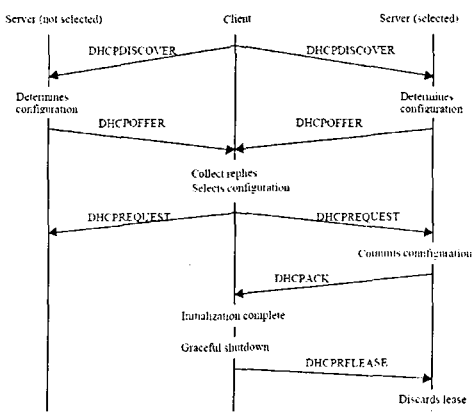

그림 1. DHCP 클라이언트의 IP 할당 받는 동작과정

Ⅲ. DHCP 메시지의 인증

3.1 DHCP의 보안 위협 및 대책

DHCP 서버와 클라이언트 사이의 IP 주소 할당 과정에 있어서 발생할 수 있는 보안 위협으로는 먼저 위장된 DHCP 서버로 DHCP 클라이언트에 대한 공격이 가능하다. 즉, 공격자가 DHCP 서버로 위장해 DHCP 클라이언트에게 IP 주소를 할당하지만, 할당하는 주소에는 잘못된 DNS, 게이트웨이 등의 정보를 포함하고 있으므로, DHCP 클라이언트는 위조된 주소 정보로 데이터를 전송한다. 또한, 위장된 DHCP 클라이언트로 DHCP 서버에 대한 공격이 가능하며, 이 외에도 DHCP 서버의 IP 주소 고갈, CPU 고갈, 네트워크 대역폭 고갈 등의 DoS(Denial of Service)공격이 가능하다.

이러한 다양한 보안 위협에 대한 대책으로 DHCP 서버의 IP주소 고갈, CPU 고갈, 네트워크 대역폭 고갈 등의 DoS 공격은 각 포트에서의 사용할 수 있는 IP 주소를 제한함으로써 대책을 세울 수 있지만, 위장된 DHCP 서버나 위장한 DHCP 클라이언트를 이용한 공격을 차단하기 위해서는 추가적인 인증 메커니즘이 요구되는데, 이러한 목적으로 RFC3118의 'Authentication for DHCP Messages'에서 DHCP 메시지의 인증 방법을 정의하고 있다[5]. 따라서, 본 논문에서는 DHCP 메시지에 대한 인증 기능을 추가하기 위해 RFC3118의 'Authentication for DHCP Messages'를 기반으로 하여 설계 및 구현하였으며, 결과적으로 DHCP 클라이언트는 인증된 DHCP 서버로부터 IP 주소를 할당받고, DHCP 서버도 인증된 DHCP 클라이언트에게 IP 주소를 할당하도록 하였다.

3.2 인증 메커니즘

본 논문에서 기술하는 DHCP 메시지 인증은 DHCP 클라이언트와 DHCP 서버의 상호인증이 가능하고, 보다 효과적인 키관리 방법과 리플레이 공격에 대해 추가적인 파라미터 설정 없이 인증 과정에서 리플레이 공격에 대한 검증이 동시에 가능하다. 이를 위해서는 DHCP 클라이언트를 DHCP 서버에 등록하는 과정이 필요하며, DHCP 서버는 DHCP 서버의 하드웨어 주소를 이용해 마스터 키(Master Key)를 생성하고, 생성된 마스터 키와 등록하고자 하는 DHCP 클라이언트의 하드웨어 주소를 사용해 비밀키를 생성하고, 생성된 비밀키를 DHCP 클라이언트에 발급해 준다. 그리고, DHCP 서버가 DHCP 클라이언트로부터 첫 번째 메시지인 DHCPDISCOVER 메시지를 수신하면, 접속한 DHCP 클라이언트에 대한 비밀키를 생성하며, DHCP 클라이언트의 접속 시간을 이용한 난수를 생성하고, 생성된 비밀키와 난수를 이용해 세션키를 생성한다. 이때, 생성된 세션키로 첫 번째 응답 메시지에 대한 HMAC값과 생성된 난수를 포함하여 첫 번째 응답 메시지

를 DHCP 클라이언트에게 전송한다.

DHCP 서버로부터 첫 번째 응답 메시지인 DHCPOFFER 메시지를 수신한 DHCP 클라이언트는 응답 메시지에 포함된 난수와 등록과정에서 DHCP 서버로부터 발급받은 비밀키를 이용해 세션키를 생성하고, 생성된 세션키로 수신한 응답 메시지에 대한 HMAC 값의 계산 및 비교를 통해 수신한 메시지를 인증한다[5-6]. 이후, DHCP 서버와 DHCP 클라이언트 사이의 전송되는 메시지는 이전에 생성한 세션키를 입력으로 해서 매 통신마다 새로운 세션키를 생성하고, 생성된 새로운 세션키로 HMAC값을 계산하여 전송하게 된다. 이때, 세션키 생성은 DHCP 클라이언트의 접속 시간을 입력으로 해서 생성되는 난수와 비밀키를 입력으로 해서 생성되며, 접속할 때 마다 달라지게 되고, 그 이후 생성되는 세션키는 이전에 생성된 세션키와 난수를 입력으로 해서 생성되므로, DHCP 클라이언트의 새로운 접속이 이루어질 때 마다 세션키가 달라져서 높은 보안성을 가짐과 동시에 리플레이 공격에 대한 방지법을 제공한다.

또한, 본 논문에서 DHCP 서버는 자신의 마스터 키만 갖고 있으며, 각각의 DHCP 클라이언트에 대한 비밀키는 갖고 있지 않는다. DHCP 클라이언트가 접속을 시도하여 첫 번째 메시지를 수신하면, 그때 접속한 DHCP 클라이언트의 하드웨어 주소와 마스터 키로 비밀키를 재생성하는 방법으로 DHCP 서버의 효율적인 키관리를 제공한다. DHCP 메시지 인증를 통한 IP 할당은 앞에서 설명한 기본적인 DHCP 동작 과정에서 옵션 사항의 추가된 인증 메커니즘에 따라 IP 주소 할당이 이루어진다. 그림2는 DHCP 서버에 DHCP 클라이언트를 등록하는 과정을 보여주며, 그림 3은 DHCP 클라이언트 중심의 메시지 인증 기능 추가 시 동작 과정, 그림 4는 DHCP 서버 중심의 메시지 인증 기능 추가 시 동작 과정을 보여준다.

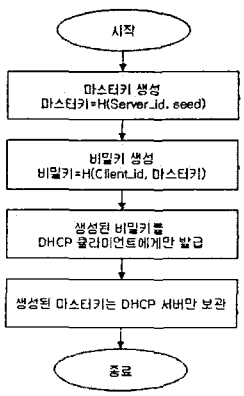

그림 2. DHCP 서버의 DHCP 클라이언트에 대한 등록 과정

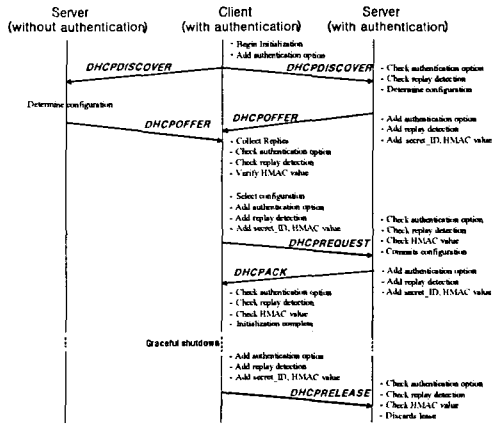

그림 3. DHCP 서버 중심의 DHCP 메시지 인증 과정

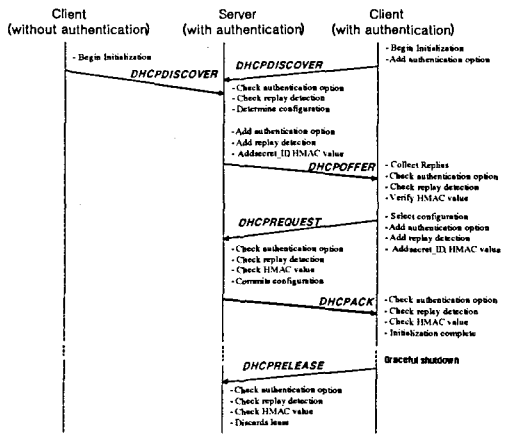

그림 4. DHCP 클라이언트 중심의 DHCP 메시지 인증 과정

IV. 홈네트워크 보안에서의 DHCP

본 논문에서 제안하는 DHCP 메시지 인증 방법은 일반적인 네트워크 관리 시스템에 적용 가능함은 물론, 홈네트워크 시스템에서 홈게이트웨이 또는 홈서버에 DHCP 기능을 추가할 경우, IP 기반으로 동작하는 홈디바이스들에 대해서는 추가적인 디바이스 인증 프로그램을 수행할 필요 없이 DHCP 메시지 인증 기능으로도 디바이스 인증 기능을 수행할 수 있을 것이다. 이는 홈서버 또는 홈게이트웨이에 등록된 홈디바이스들만 DHCP 서버로부터 IP를 할당 받을 수 있도록 하며, 등록되지 않은 홈디바이스들은 IP를 할당 받지 못하므로 더 이상의 통신이 불가능하게 된다. 또한, DHCP 메시지 인증 기능은 옵션 사항으로 처리할 수 있으므로, 먼저 DHCP 기능을 수행하여 IP 할당을 하고, 이후 사용자 인증과정을 통해 홈네트워크 접속을 허용 또는 차단할 수도 있다.

따라서, 홈네트워크에서 DHCP 메시지 인증 기능을 적용함에 있어서, 디바이스 인증 또는 사용자 인증 기능에 적용하는 것은 홈서버 또는 홈게이트웨이의 DHCP 서버의 환경 설정에 따라 쉽게 적용할 수 있을 것이다.

V. 결론

본 논문에서 제안하는 DHCP 메시지 인증 방법은 IP할당 시, 위장한 DHCP 서버 또는 위장한 DHCP 클라이언트로 인한 공격으로부터 피해를 막을 수 있으며, 동시에 리플레이 공격에 대한 피해도 막을 수 있는 효과가 있다. 또한, DHCP 서버는 자신의 마스터 키 하나만 가지고, 각 클라이언트에 대한 비밀키는 저장할 필요 없이, 각 클라이언트가 접속하는 시점에서 재생성하는 방법을 사용해 보다 효율적인 키관리 방법을 제공한다. 따라서, 향후 홈네트워크에서 디바이스 인증 기능에 적용하고자 한다면 IP 기반의 홈디바이스인 경우에 대해서는 충분히 적용 가능하리라 예상된다.

참고문헌

[1] Kaaumasa Kobayashiand Suguru Yamaguchi, "Network Access Control for DHCP Environment", *INET97 Proceedings*, 1997.

[2] 한종욱, 김도우, 이윤경, 주홍일, 남택용, 장종수, "안전한 홈네트워크 구축을 위한 보안요구사항", 한국정보처리학회지, 2004.05 v.11, n.3, pp.38-45.

[3] 한종욱, 김도우, 이윤경, 주홍일, 박지혜, "홈네트워크 사용자 인증메커니즘", 한국해양정보통신학회 2004년도 추계종합학술대회, 2004.10 Vol.8, No.2 .

[4] R. Droms, "Dynamic Host Configuration Protocol", *RFC 2131*, March 1997.

[5] R. Droms, W. Arbaugh, "Authentication for DHCP messages", *RFC 3118*, June 2001.

[6] Mitch Tulloch, "DHCP Server Security (Part 1)", *Articles::Misc Network Security*, Jul 2004.